MAT0265 - Grupos

Prova 1

Pedro Gigeck Freire
10737136

21/10/2020

Questão 1

Seja G um grupo, $G \neq \{e\}$. Mostre que se G não possui subgrupos não triviais, então G é finito e cíclico de ordem prima.

Suponha que G não possui subgrupos não triviais.

- Vamos mostrar que G é cíclico:

Seja $a \in G$, com $a \neq e$. (Sabemos que existe pois $G \neq \{e\}$).

Sabemos, do resultado visto na aula 3 (09/09) que

$\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$ é subgrupo de G.

Como $\langle a \rangle \neq \{e\}$, e G tem apenas subgrupos triviais, então

$\langle a \rangle = G$.

Portanto G é cíclico.

Além disso, note que todo elemento $a \in G$, com $a \neq e$ é gerador.

- Vamos mostrar que G é finito.

Seja $a \in G$, com $a \neq e$.

Conforme acabamos de mostrar, temos que a e a^2 são geradores de G.

Ou seja

$\langle a \rangle = \langle a^2 \rangle = G$.

Portanto, temos que

$a \in \langle a^2 \rangle \Rightarrow$

$a = (a^2)^i$, para algum $i \in \mathbb{Z}$

Então

$$a = a^{2i} \Rightarrow a^{2i-1} = e$$

Suponha, por absurdo, que G seja infinito

Como $\underline{a}$ é gerador, $\underline{a}$ não tem ordem finita,

Portanto

$$a^{2i-1} = e \Rightarrow 2i - 1 = 0 \Rightarrow i = 1/2 \notin \mathbb{Z} \quad \text{(absurdo)}.$$

Logo, G é finito.

Seja $p = |G|$ a ordem de G.

- Vamos mostrar que p é primo:

Suponha, por absurdo, que p não é primo.

Então p pode ser decomposto em

$$p = q_1 q_2 \quad , \text{com } q_1, q_2 \in \mathbb{Z} \quad , \quad 1 < q_1 \leq q_2 < p.$$

Portanto, sendo

$a \in G$ gerador,

Então a ordem de $\underline{a}$ é p.

Logo

$$a^p = e \Rightarrow a^{q_1 q_2} = e \Rightarrow (a^{q_1})^{q_2} = e$$

Mas, a^{q_1} também é gerador, então a ordem de a^{q_1} é p.

Mas $q_2 < p$ e $(a^{q_1})^{q_2} = e$, absurdo, pois p deveria ser o menor inteiro tal que $a^p = e$.

Com isso, de fato $|G| = p$ é primo.